

# EXHIBIT C

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION**

DONNA CURLING, *et al.*

*Plaintiffs,*

v.

BRAD RAFFENSPERGER, *et al.*,

*Defendants.*

CIVIL ACTION

FILE NO. 1:17-cv-2989-AT

**DECLARATION OF THERESA PAYTON**

Pursuant to 28 U.S.C. § 1746, I, Theresa Payton, make the following declaration:

**I. BACKGROUND**

1.

My name is Theresa Payton. I am over the age of 21 years, and I am under no legal disability which would prevent me from giving this declaration.

2.

I am the Chief Executive Officer of Fortalice Solutions. Fortalice Solutions is a full-service cybersecurity company that offers businesses and governments a full suite of cybersecurity services, including cybersecurity assessments, vendor

assessments, red teaming and penetration testing, review of cybersecurity policies and procedures, and cyber incident response and analysis.

3.

Prior to founding Fortalice, I was Chief Information Officer for The Office of Administration, Executive Office of the President at the White House from 2006-2008, overseeing all information technology and information security functions. I am the co-author of numerous books and articles regarding cyber-security, including *Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family* and *Protecting Your Internet Identity: Are You Naked Online?* I was named one of the 25 Most Influential People in Security by Security Magazine.

## **II. CYBER RISK ASSESSMENT OF SECRETARY OF STATE SYSTEMS**

4.

The Georgia Secretary of State's Office ("SOS") has retained Fortalice to provide cybersecurity assessments of SOS networks and vendors, including elections related networks. We have also conducted penetration testing of these networks,

reviewed cybersecurity policies and procedures, and from time to time, conducted cyber-incident response and analysis. Our incident response and analysis activities involve reviewing log files from certain servers and applications to determine what activity has occurred and whether any attempts to penetrate systems have been successful, attempt to isolate malicious activity, and attempt to determine where any malicious activity originates.

5.

Between June 2017 and September 2017, Fortalice Solutions completed an initial cyber risk assessment of the SOS IT environment. Fortalice Solutions then reassessed the SOS IT environment in November 2018, including a red team penetration testing effort. Between November 2017 and February 2018, Fortalice Solutions conducted, at the request of SOS, a cyber risk assessment of PCC Technology, Inc. (“PCC”), a company delivering managed services to the IT environment of election related systems and services for SOS.

6.

In the November 2018 reassessment, Fortalice determined that SOS was documenting many operations correctly and had a proper mindset oriented towards

iterative improvement of cybersecurity. During the on-network red team penetration test, the Fortalice team was stymied by certain controls already in place at the SOS network. For instance, it is a common practice for a red team to access networks as part of rules of engagement by guessing passwords. In the case of SOS, Fortalice was unable to access the SOS network through password guessing. The next method typically deployed during a red team assessment is to deploy social engineering schemes via email and other methods. In the case of SOS, Fortalice sent out a phishing email. The phishing email sent by Fortalice had some success in being delivered to end-users. We find that we always have a user that falls for social engineering in our tests, so this is common. However, despite some users taking the bait, Fortalice did not achieve any command- and-control (C2) callbacks as a result. The SOS implementation of Dell SecureWorks successfully alerted on red team attempts to deploy C2 frameworks inside the SOS network.

## 7.

Of the risks outlined in the 2017 report, Fortalice found that as of the November 2018 reassessment, three risks had been remediated with compensating controls and another three were in process of being fixed.

8.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 10th day of July, 2019.



---

THERESA PAYTON